CLAIMS

1. A transaction verification system for use in verifying transactions between computers connected by a computer network, the system comprising fingerprint means operable in association with at least one first computer of the network to seek information relating to the first computer in order to create a group of data to serve as a fingerprint which is substantially unique to the first computer, and to provide the fingerprint for transmission to a second computer when the first computer is operated to initiate a transaction, to allow the source of the transaction initiation to be substantially uniquely identified.

2. The system of claim 1, wherein the fingerprint includes data which identifies components of the system of the first computer.

3. The system of claim 2, wherein the fingerprint includes data relating to hardware present within the first computer, or to software present within the first computer.

4. The system of claim 2, wherein the fingerprint further includes data input by the user in response to a prompt provided by the fingerprint means.

5. The system of claim 1, wherein the second computer is operable to store the fingerprint in association with details of the transaction, for future reference to identify the first computer.

6. The system of claim 5, wherein the second computer is operable to provide a message confirming that the fingerprint has been stored and authorising the transaction to proceed.

7. The system of claim 5, wherein the second computer is operable to store, with the fingerprint, the route by which the fingerprint travelled across the network, including details of any servers through which the fingerprint passed.

8. The system of claim 1, wherein the second computer is operable to use

the fingerprint to provide active verification of the validity of the transaction.

9. The system of claim 5, wherein the second computer is operable to effect a payment in response to receiving details of the transactions.

10. The system of claim 5, wherein the second computer incorporates a database operable to identify the payment required in relation to the transaction.

11. The system of claim 5, wherein the second computer contains stored fingerprint data for comparison with a fingerprint created at the time of a transaction, for authorising the transaction in accordance with the result of the comparison.

12. The system of claim 1, wherein the first computer comprises transaction means operable to create a transaction request identifying a required transaction, and means operable to transmit the transaction request over the network to another computer with which the transaction is to be conducted.

13. The system of claim 12, wherein the said another computer is a third computer.

14. The system of claim 13, wherein the system comprises a plurality of first computers able to initiate transactions as aforesaid, a plurality of third computers operable to execute transactions requested by the first computers, and a second computer common to at least some of the first and third computers and operable to receive a fingerprint associated with a transaction, and to store that fingerprint as verification of that transaction.

15. The system of claim 12, wherein the system comprises a plurality of first computers able to initiate a transaction as aforesaid, and a plurality of further computers, at least one of which is operable to execute transactions requested by the first computers and also to receive a fingerprint associated with each transaction, and to store that fingerprint as verification of that transaction.

16. The system of claim 1, wherein a transaction includes the purchase of data which is downloaded to the first computer over the network.

17. The system of claim 1, wherein the fingerprint means comprise software operable as aforesaid.

18. The system of claim 1, wherein the, or each of the computers which are connected to the network and are operable to complete transactions requested by the first computer are operable to download the fingerprint means to the first computer.

19. The system of claim 18, wherein the fingerprint means is downloaded as part of a dialogue by which the parameters of the transaction are set by operation of the first computer, and wherein the fingerprint means are required to be run to create a fingerprint as aforesaid, before the transaction takes place.

20. A computer comprising means operable to connect the computer to a network over which transactions can be executed, the computer further comprising fingerprint means operable to seek information relating to the computer in order to create a group of data to serve as a fingerprint which is substantially unique to the computer, and operable when the computer is operated to initiate a transaction, to provide the fingerprint for transmission to a second computer to allow the source of the transaction initiation to be uniquely defined.

21. The computer of claim 20, wherein the fingerprint includes data which uniquely identifies components of the system of the first computer.

22. The computer of claim 21, wherein the fingerprint includes data relating to hardware present within the first computer.

23. The computer of claim 21 or 22, wherein the fingerprint includes data relating to software present within the first computer.

24. The computer of claim 21, wherein the fingerprint includes data input by the user in response to a prompt provided by the fingerprint means.

25. The computer of claim 20, wherein the said computer comprises transaction means operable to create a transaction request identifying a required transaction, and means operable to transmit the transaction request over the network to another computer with which the transaction is to be conducted.

26. The computer of claim 20, wherein a transaction includes the purchase of data which is downloaded to the said computer over the network.

27. The computer of claim 20, wherein the fingerprint means comprise software operable as aforesaid.

28. A computer comprising means operable to connect the computer to a network over which transactions can be executed, the computer comprising means operable to receive fingerprint data identifying a computer involved in the transaction, and to store the fingerprint data in association with details of the transaction for future reference to identify the said computer involved in the transaction.

29. The computer of claim 28, wherein the fingerprint includes data which uniquely identifies components of the system of the first computer.

30. The computer of claim 29, wherein the fingerprint includes data relating to hardware present within the first computer, or to software present within the first computer.

31. The computer of claim 28, wherein the fingerprint includes data input by the user in response to a prompt provided by the fingerprint means.

32. The computer of claim 28, wherein the computer is operable to provide a message confirming that the fingerprint has been stored and authorising the

transaction to proceed.

33. The computer of claim 28, the computer being operable to store, with the fingerprint, the route by which the fingerprint travelled across the network, including details of any servers through which the fingerprint passed.

34. The computer of claim 28, wherein the computer is operable to use the fingerprint to provide active verification of the validity of the transaction.

35. The computer of claim 28, wherein the computer is operable to effect a payment in response to receiving details of the transaction.

36. The computer of claim 28, wherein the computer incorporates a database operable to identify the payment required in relation to the transaction.

37. The computer of claim 28, wherein the computer contains stored fingerprint data for comparison with a fingerprint created at the time of a transaction, for authorising the transaction in accordance with the result of the comparison.

38. The computer of claim 28, wherein the transaction includes the purchase of data which is downloaded over the network.

39. A computer comprising means operable to connect the computer to a network over which transactions can be executed, and further comprising means operable to receive a transaction request by means of the network, means operable to execute the requested transaction, means operable to receive verification that a fingerprint has been stored in relation to the transaction, and means operable to prevent execution until verification has been received, the fingerprint including information which is substantially unique to the computer requesting the transaction.

40. The computer of claim 39, wherein the fingerprint includes data which uniquely identifies components of the system of the first computer.

41. The computer of claim 39, wherein the fingerprint includes data relating to hardware present within the first computer, or to software present within the first computer.

42. The computer of claim 39, wherein the fingerprint includes data input by the user in response to a prompt provided by the fingerprint means.

43. The computer of claim 39, wherein the transaction includes the purchase of data which is downloaded over the network.

44. The computer of claim 39, wherein the computer is operable to download fingerprint means to a computer requesting a transaction, the fingerprint means being operable to seek information relating to the initiating computer, in order to create a group of data to serve as a fingerprint which is substantially unique to the initiating computer.

45. The computer of claim 44, wherein the fingerprint means is downloaded as part of a dialogue by which the parameters of the transaction are set by operation of the initiating computer.

46. A method of verifying transactions between computers connected by a computer network, in which a group of data is created to serve as a fingerprint which is substantially unique to a first computer, and the fingerprint is provided to a second computer when the first computer is operated to initiate a transaction, to allow the source of the transaction initiation to be substantially uniquely defined.

47. The method of claim 46, wherein the fingerprint includes data which identifies components of the system of the first computer.

48. The method of claim 47, wherein the fingerprint includes data relating to hardware present within the first computer, or to software present within the first computer.

49. The method of claim 47, wherein the user is prompted to provide further data to be included in the fingerprint.

50. The method of claim 46, wherein the fingerprint is stored in association with details of the transaction, for future reference to identify the first computer.

51. The method of claim 50, wherein a message is provided to confirm that the fingerprint has been stored and authorising the transaction to proceed.

52. The method of claim 50, wherein the route by which the fingerprint travelled across the network is stored with the fingerprint, including details of any servers through which the fingerprint passed.

53. The method of claim 46, wherein the fingerprint is used to provide active verification of the validity of the transaction.

54. The method of claim 50, wherein payment is effected in response to receiving details of the transactions.

55. The method of claim 50, wherein fingerprint data is stored for comparison with a fingerprint created at the time of a transaction, for authorising the transaction in accordance with the result of the comparison.

56. A data storage medium comprising software operable to seek information relating to the computer on which the software is running, and to create a group of data serving as a fingerprint which is substantially unique to the said computer, the software being further operable to provide the fingerprint for transmission to a second computer when the first computer is operated to initiate a transaction, to allow the source of the transaction initiation to be uniquely identified.

57. The data storage medium of claim 56, wherein the software is operable to create a fingerprint which includes data which uniquely identifying components

of the system of the first computer.

58. The data storage medium of claim 57, wherein the fingerprint includes data relating to hardware or software present within the first computer.

59. The data storage medium of claim 57, wherein the fingerprint includes data input by the user in response to a prompt provided by the fingerprint means.

60. Software operable to seek information relating to the computer on which the software is running, and to create a group of data serving as a fingerprint which is substantially unique to the said computer, the software being further operable to provide the fingerprint for transmission to a second computer when the first computer is operated to initiate a transaction, to allow the source of the transaction initiation to be uniquely identified.

61. The software of claim 60, operable to create a fingerprint which includes data which uniquely identifying components of the system of the first computer.

62. The software of claim 61, wherein the fingerprint includes data relating to hardware or software present within the first computer.

63. The software of claim 61, wherein the fingerprint includes data input by the user in response to a prompt provided by the fingerprint means.

64. A transaction verification system substantially as described above, with reference to the accompanying drawings.